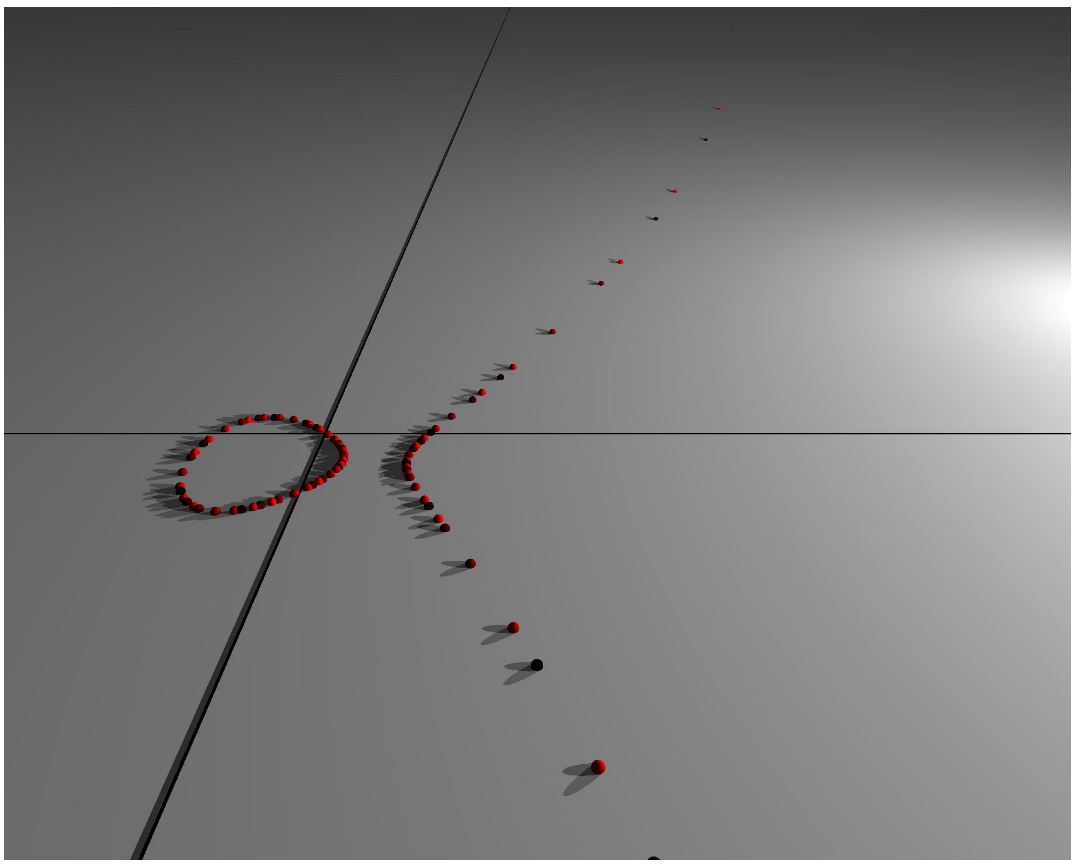
MVHS NUMBER THEORY GROUP NOTES

MICHAEL MUSTY



"To think deeply of simple things." Arnold E. Ross

1. October 11 2009 - October 17 2009

Introduction. The *MVHS number theory group* is an after school math program at Merrimack Valley High School intended to give students an idea about how and why mathematics is used outside of the high school curriculum. The program is centered around patterns and symmetries arising from the *integers*

$$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$$

The program is based on this so called *number theory* for various reasons. Firstly, number theory can be intuitive, hands on, and exploratory. Secondly, there are numerous real life applications of number theory which students can be exposed to in this exploratory way. The MVHS number theory group is somewhat inspired (though in no way officially affiliated) by *The Ross Program* at Ohio State University (http://www.math.ohio-state.edu/ross/) and *PROMYS* at Boston University (http://www.promys.org/). For more information about related programs check out the *American Mathematical Society Epsilon Fund* (http://www.ams.org/). Mike Musty can be reached by email at `mmusty@mv.k12.nh.us` (or more reliably at `musty@math.mcgill.ca`). The website for the group is

`numbertheorygroup.blogspot.com`

Check there for updates to the notes as well as announcements and stuff... Anyways, let's begin!

The Integers (also known as $\mathbb{Z}$). In its most elementary form, a *number* can be represented as a collection of identical objects as follows

$$\begin{aligned} 1 &= \bullet \\ 2 &= \bullet\ \bullet \\ 3 &= \bullet\ \bullet\ \bullet \\ 4 &= \bullet\ \bullet\ \bullet\ \bullet \\ 5 &= \bullet\ \bullet\ \bullet\ \bullet\ \bullet \\ &\vdots \end{aligned}$$

When numbers are viewed in this way there are certain *operations* which can take two such numbers and create a single number. One operation is *addition.* Addition takes two numbers

$$\begin{aligned} a &= \overbrace{\bullet\ \cdots\ \bullet}^{a} \\ b &= \overbrace{\bullet\ \cdots\ \bullet}^{b} \end{aligned}$$

and creates a new number

$$a + b = \overbrace{\bullet\ \cdots\ \bullet}^{a+b}$$

For example,

$$\bullet\ \bullet\ \bullet + \bullet\ \bullet\ \bullet\ \bullet\ \bullet = \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet\ \bullet$$

Seems simple enough, after all we have been doing this practically since birth! Another slightly more complicated operation is *multiplication*. Multiplication takes two numbers

$$\begin{aligned} a &= \overbrace{\bullet \quad \cdots \quad \bullet}^{a} \\ b &= \overbrace{\bullet \quad \cdots \quad \bullet}^{b} \end{aligned}$$

and creates a new number

$$a \times b = \overbrace{\begin{matrix} \bullet & \cdots & \bullet \\ \vdots & \ddots & \vdots \\ \bullet & \cdots & \bullet \end{matrix}}^{\text{An } a \text{ row by } b \text{ column rectangle}}$$

Using the same example as with addition,

$$\bullet \quad \bullet \quad \bullet \times \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet = \begin{matrix} \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet & \bullet \end{matrix}$$

Yet this is not how we view numbers in our everyday lives. Instead we use the symbols $1, \ldots, 9$ to represent the collections $\bullet$ through $\bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet \quad \bullet$ respectively. But at ten something funny happens. Instead of simply having another symbol for ten, we take the symbol 1 and move it left a single space. To keep track of how far left we introduce another symbol *zero* as a place holder. If we continue in this fashion (i.e. continually moving left using the place holder zero) we can represent arbitrarily large numbers in a much less cumbersome way. This is the aptly named *base* 10 *number system* or *decimal system* that we use today. Why 10 was chosen as a base is anyone's guess (we have ten appendages on our hands...). For a historical account of this question see [OA66] and [Ore67] in the reference section.

In the decimal system, every number is written as a sum of powers of ten, i.e. a *polynomial in the base* 10. As an example we have

$$341 = 3 \cdot 10^2 + 4 \cdot 10^1 + 1 \cdot 10^0$$

and it only takes a minute to convince yourself that the numbers representable as collections of dots are the same as those representable as sums of *positive* powers of ten.

Exercise 1.1. Convince yourself that the numbers representable as collections of dots are the same as those representable as sums of positive powers of ten.

Now what about addition and multiplication in the decimal system? Are they the same as the methods described above with the collections of dots? Indeed the two are identical, and the reason we introduced numbers as collections of dots in the first place was to realize the motivation behind the addition and multiplication we are so accustomed to today.

Exercise 1.2. Add and multiply 43 with 126 in the two different ways to convince yourself of the previous statement.

These first two exercises may seem very basic and obvious, but it is important to keep in mind what motivates the things we study (especially as things get more complicated). To prove this point, the following exercise is very similar to the previous one, but turns out to be much more difficult.

Exercise 1.3 (Challenge). Look up *Karatsuba Multiplication* and convince yourself that it accomplishes the same task as ordinary multiplication. Do the same for *Schönhage-Strassen Multiplication*.

Going back to viewing numbers as "polynomials," we can also understand the reasoning behind polynomial multiplication. Using the numbers from the exercise,

$$126 = 1 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0$$
$$43 = 0 \cdot 10^2 + 4 \cdot 10^1 + 3 \cdot 10^0$$

we see that doing the multiplication

$$126 \cdot 43 = 5418$$

is precisely the same as "FOILING" the polynomials

$$(1 \cdot x^2 + 2 \cdot x^1 + 6 \cdot x^0) \cdot (0 \cdot x^2 + 4 \cdot x^1 + 3 \cdot x^0)$$

and substituting 10 in for x afterward. To see this observe the following equalities.

$$\begin{aligned}
5418 &= 126 \cdot 43 \\
&= \left(1 \cdot 10^2 + 2 \cdot 10^1 + 6 \cdot 10^0\right) \cdot \left(4 \cdot 10^1 + 3 \cdot 10^0\right) \\
&= 1 \cdot 10^2 \cdot 4 \cdot 10^1 + 1 \cdot 10^2 \cdot 3 \cdot 10^0 \\
&+ 2 \cdot 10^1 \cdot 4 \cdot 10^1 + 2 \cdot 10^1 \cdot 3 \cdot 10^0 \\
&+ 6 \cdot 10^0 \cdot 4 \cdot 10^1 + 6 \cdot 10^0 \cdot 3 \cdot 10^0 \\
&= 4 \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10^2 + 6 \cdot 10^1 + 24 \cdot 10^1 + 18 \cdot 10^0 \\
&= 4 \cdot 10^3 + 11 \cdot 10^2 + 30 \cdot 10^1 + 18 \cdot 10^0 \\
&= 4 \cdot 10^3 + \left(1 \cdot 10^1 + 1 \cdot 10^0\right) \cdot 10^2 + \left(3 \cdot 10^1 + 0 \cdot 10^0\right) \cdot 10^1 + \left(1 \cdot 10^1 + 8 \cdot 10^0\right) \cdot 10^0 \\
&= 4 \cdot 10^3 + 1 \cdot 10^3 + 1 \cdot 10^2 + 3 \cdot 10^2 + 0 \cdot 10^0 + 1 \cdot 10^1 + 8 \cdot 10^0 \\
&= 5 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10^1 + 8 \cdot 10^0 \\
&= 5418
\end{aligned}$$

Exercise 1.4. What do the above equalities tell us about the relationship between the multiplication of numbers $126 \cdot 43$ and the multiplication of polynomials $(x^2 + 2 \cdot x \cdot 6) \cdot (4 \cdot x + 3)$? Create your own example to exhibit this relationship. Is it obvious that this relationship is *always* true?

And so we see that there is a correspondence between polynomials of the form

$$c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \cdots + c_2 \cdot x^2 + c_1 \cdot x + c_0$$

and base ten numbers

$$c_n \cdot 10^n + c_{n-1} \cdot 10^{n-1} + \cdots + c_2 \cdot 10^2 + c_1 \cdot 10 + c_0$$

given by simply interchanging

$$x \longleftrightarrow 10$$

Exercise 1.5. For what values of $c_0, c_1, \ldots, c_{n-1}, c_n$ (these are called *coefficients*) does this correspondence make sense? The polynomial

$$9 \cdot x^3 + 12 \cdot x^2 + 144 \cdot x + 7$$

corresponds to what base ten number? Does every number correspond to some polynomial? Are there any numbers which correspond to more than one polynomial? Is there a restriction on the coefficients which makes every number correspond to *exactly* one polynomial?

The Language of Computers and Other Bases. Suppose we wanted to add or multiply two numbers written in base ten (say 1567 and 895). Most of us would just reach for our handy dandy graphics calculator and the magical answer of 1402465 would appear on our screen. We do this of course because it is faster. We *know* how a calculator gets the answer. Any one of us could have very well written the numbers one on top of the other and multiplied them together in the same way as any computer. Right? Wrong! On the contrary, computers do *not* work in base ten but rather most commonly work in base two also known as the *binary system.* To demonstrate how a computer adds and multiplies these two numbers, we must first convert them from base 10 to base 2. To make this easier we first write out some powers of 2.

$$\begin{aligned}
2^0 &= 1\\
2^1 &= 2\\
2^2 &= 4\\
2^3 &= 8\\
2^4 &= 16\\
2^5 &= 32\\
2^6 &= 64\\
2^7 &= 128\\
2^8 &= 256\\
2^9 &= 512\\
2^{10} &= 1024\\
2^{11} &= 2048
\end{aligned}$$

To write 1567 in base 2 we first find the largest power of 2 that does not exceed 1567. From the above table we find that it is $2^{10} = 1024$. We can now write

$$1567 = 1 \cdot 2^{10} + (1567 - 1024) = 1 \cdot 2^{10} + 543$$

To finish the process we must now convert 543 into a sum of powers of 2. Again from the table we find that the largest power of 2 not exceeding 543 is $2^9 = 512$ so we can continue to write

$$1567 = 1 \cdot 2^{10} + 1 \cdot 2^9 + (543 - 512) = 1 \cdot 2^{10} + 1 \cdot 2^9 + 31$$

Continuing in this manner gives us

$$\begin{aligned}
1567 &= 1 \cdot 2^{10} + 1 \cdot 2^9 + 31 \\
&= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^4 + 15 \\
&= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^4 + 1 \cdot 2^3 + 7 \\
&= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 3 \\
&= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \\
&= 1 \cdot 2^{10} + 1 \cdot 2^9 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0
\end{aligned}$$

Using this we can now write 1567 in base 10 as 11000011111 in base 2.

Exercise 1.6. Why are there 4 zeros in the base 2 representation of 1567? Convert 895 base 10 to base 2. Why is the answer 1101111111?

Exercise 1.7. We know that $1567 + 895 = 2462$ all in base 10. How would we go about adding $11000011111 + 1101111111$ in base 2? Do we get the same answer?

Exercise 1.8. Multiply $1567 \cdot 895$ in base 10. Multiply $11000011111 \cdot 1101111111$ in base 2. Again, in what sense are the answers the same? Be patient with this exercise, it will take some paper and some patience. If you find it too tedious or difficult use smaller numbers to get the idea.

Computers use the binary system because at its most elementary level, a computer is a bunch of on/off switches corresponding to the zeros and ones of the binary system. But if we forget about computers for a second, there was nothing special about converting numbers to base 2 that cannot be done for other bases. In a similar way we can convert numbers to base 3 (the *ternary* system) and higher.

Exercise 1.9. Convert 1567 and 895 from base 10 to base 3 and verify that addition and multiplication work analogously (or create your own example).

Exercise 1.10. There are many ways to convert a number in base a of the form

$$c_n \cdot a^n + c_{n-1} \cdot a^{n-1} + \cdots + c_2 \cdot a^2 + c_1 \cdot a + c_0$$

to a number in base b of the form

$$d_n \cdot b^m + d_{m-1} \cdot b^{m-1} + \cdots + d_2 \cdot b^2 + d_1 \cdot b + d_0$$

We worked through one way above in the notes, can you think of any other ways? Can you think of any shortcuts or tricks [1] ?

Some Observations in Base 10. Does 9 divide 99? Does 9 divide 999? What about an arbitrarily long string of nines $999 \cdots 9$? The answer to all of these questions is yes, but why? Consider the number 999. We know from before that this means

$$\begin{aligned}
999 &= 9 \cdot 100 + 9 \cdot 10 + 9 \cdot 1 \\
&= 9 \cdot (100 + 10 + 1) \\
&= 9 \cdot 111
\end{aligned}$$

[1] Mathematicians are notoriously lazy. They are always looking for the quickest and easiest way to do everything.

In the same way,

$$\begin{aligned}\overbrace{999\cdots 9}^{n\text{ times}} &= 9\cdot 10^n + 9\cdot 10^{n-1} + \cdots + 9\cdot 10^2 + 9\cdot 10 + 9\cdot 1\\ &= 9\cdot\left(10^n + 10^{n-1} + \cdots 10^2 + 10 + 1\right)\\ &= 9\cdot \overbrace{111\cdots 1}^{n\text{ times}}\end{aligned}$$

Taking this one step further we can characterize *all* positive integers which are divisible by 9 (not just numbers which are strings of nines). Take a number written in base ten as $abcd$, i.e.

$$abcd = a\cdot 1000 + b\cdot 100 + c\cdot 10 + d$$

We can rewrite this number as

$$\begin{aligned}abcd &= a\cdot 1000 + b\cdot 100 + c\cdot 10 + d\\ &= (999\cdot a + 99\cdot b + 9\cdot c) + (a+b+c+d)\end{aligned}$$

We just saw that 9 divides any string of nines, so in particular $9, 99$, and 999 are all divisible by 9. This means that 9 divides

$$999\cdot a + 99\cdot b + 9\cdot c$$

But in order for $abcd$ to be divisible by 9 we need $(a+b+c+d)$ to be divisible by 9 as well. Does it matter that we only used a number with four digits $abcd$? Does this *prove* that base ten numbers divisible by nine are precisely those whose digits sum to a multiple of 9?

Exercise 1.11. Is the base ten number 123456789 divisible by nine? What if we switch the digits around? How many different base ten numbers can we get by switching around (also known as *permuting*) the digits of 123456789? Why are they all divisible by nine?

Exercise 1.12. Can you think of a similar test to tell if a base ten number is divisible by 11? As a hint, we can write the same number $abcd$ as

$$abcd = (1001\cdot a + 99\cdot b + 11\cdot c) + (-a + b - c + d)$$

Are $1001, 99$, and 11 all divisible by 11? Does it matter that we used a four digit number?

Exercise 1.13. (Challenge) Do you have any conjectures about numbers divisible by 7? More to come later...

Just to note, some of the material from this subsection comes from [OA66, page 13].

A Combinatorial Interpretation. Remember our conversation about a computer being a bunch of on/off switches? Looking at numbers in a slightly different light gives us a way to count various combinations of switches. Suppose, for example, we have a row of three on/off switches (a very simple computer!) and we want to know how many different *combinations* this set of switches has. Examples of combinations are `(off,off,off)`, `(on,on,on)`, `(on, off, on)`, etc. We consider the order to be important and thus count combinations like `(on, off, on)` and `(on, on, off)` as being different from each other.

Exercise 1.14. There are 8 combinations for the row of three on/off switches. Can you list them? How does the number of combinations relate to the number 111 written in base 2? What if we have 4 switches instead of three? Does the number 1111 in base 2 relate in the same way as before? What if we have n on/off switches?

Exercise 1.15. Go back to the example with three switches, but instead of the switches being on/off switches suppose they can change between 3 different positions or *states*. Is there an analog of the previous exercise to numbers in base 3? Can we extend this idea to switches with b different states (for arbitrarily large b) and numbers written in base b? Perhaps it will help to first consider the analog in base 10.

Exercise 1.16. Poker.............

2. October 18 2009 - October 24 2009

Properties of $\mathbb{Z}$. Perhaps the greatest mathematician of the 20th century David Hilbert [2] said,

Man muss immer mit den einfachsten Beispielen anfangen

which is the German equivalent of saying, "One must begin with the simplest examples." In some sense this is what we are doing when we study the integers $\mathbb{Z}$. When we think of these numbers they are simple. All we have to do is count to nine again and again. Yet there are many questions about $\mathbb{Z}$ which we cannot currently answer, which we may never even be able to answer.

We do, however, know many things about $\mathbb{Z}$. Indeed we have been learning about them since we started school, maybe before. Here are some questions to help you remember what you already know about the integers.

Exercise 2.1 (Commutative Property of Addition and Multiplication).

Exercise 2.2 (Identities).

Exercise 2.3 (Inverses).

Exercise 2.4 (Distributive Property).

Exercise 2.5 (Associative Property).

These properties seem somewhat boring and trivial, but they are important for two reasons. The first reason is that it is important to learn how to *prove* something rigorously in the language of mathematics, and these properties give students a place to start learning this art. Secondly, these properties describe something we are trying to understand (namely $\mathbb{Z}$) and are fundamental to the way in which we proceed to study $\mathbb{Z}$. For instance, once we know that $\mathbb{Z}$ is commutative, we don't have to worry about the order of multiplication and addition. We would go about studying $\mathbb{Z}$ much differently if the integers were non-commutative.

[2] Hilbert helped Einstein through the hairiest mathematics of the theory of *general relativity*, but is most well-known for his plan in the early 1900s to completely *formalize* mathematics. *Hilbert's Program* consisted of a set of problems to "lead mathematicians into the next century." At least two of these problems have been shown to be *undecidable* (i.e. there exists no proof nor counter proof) in our current system of mathematics. Given the extent to which mathematics has been spread out, it is unlikely there will ever be another person with such a deep all-encompassing view of the subject.

Whenever we have a way to describe a mathematical object (in our case we have a list of properties which are true about $\mathbb{Z}$) we can ask whether or this description has enough information for us to distinguish our object from other mathematical objects. In our case, the above properties do NOT give us a way to tell $\mathbb{Z}$ apart from other mathematical objects. There are actually infinitely many mathematical objects that share the same properties with $\mathbb{Z}$ above [3]. There is, however, one property about $\mathbb{Z}$ which sets it apart from many such objects. It is called *The Fundamental Theorem of Arithmetic*.

Exercise 2.6 (The Fundamental Theorem of Arithmetic). We call a number *prime* (not equal to 1) if its only divisor is ± 1. Is 2 prime? What about $3, 5, 7, 11, 13, 101$? We say a number n *factors* into divisors a and b if $n = a \cdot b$. Does 6 factor into prime numbers? What about $30, 210, 2310, 30030$? Write the factorizations below.

$$\begin{aligned} 6 &= \\ 30 &= \\ 210 &= \\ 2310 &= \\ 30030 &= \end{aligned}$$

Why did I have you write these numbers? Can every integer be factored as a product of primes? In what sense is this product *unique*? Factor the numbers ± 561 below.

$$\begin{aligned} +561 &= \\ -561 &= \end{aligned}$$

Resort back to the properties in previous exercises about the integers if needed. Should order matter when we factor an integer into a product of prime numbers? In regards to previous exercises, what is special about ± 1? What is special about ± 1 in this exercise?

IF YOU ARE READING THIS PART AND HAVE NOT DONE THE PREVIOUS EXERCISE, THEN DO THE PREVIOUS EXERCISE BEFORE READING ON. *The Fundamental Theorem of Arithmetic* states that every integer a can be written as a product

$$a = p_1 \times p_2 \times \cdots \times p_n$$

Where the numbers $p_1, p_2, \cdots, p_n$ are prime numbers. Moreover, it states that this product is *unique* if we don't consider multiplying by ± 1 or reordering the factors to be a *different* product. At this point we can again ask whether or not the fundamental theorem distinguishes $\mathbb{Z}$ from every other object we can study and of course the answer is no, but just as before it helps tell us how to proceed. The reason $\mathbb{Z}$ is interesting is because we can't answer yes to this question. If we could, then in some sense we would know everything about $\mathbb{Z}$ and it would no longer be interesting. As far as proving the fundamental theorem goes, this is beyond the scope of what we are trying to do at the moment. But the statement will shed much light on what we do in the next section.

[3] We may not know of any others at the moment, but we will. Such objects are called *commutative rings with identity*.

The Division Algorithm. Suppose now that we have two integers n and m. We know from the fundamental theorem of arithmetic that

$$n = p_1 \cdots p_r$$
$$m = q_1 \cdots q_s$$

where the numbers $p_1, \cdots, p_r, q_1, \cdots, q_s$ are prime, and the products are unique (in what sense?). As an example

$$561 = 3 \cdot 11 \cdot 17$$
$$2145 = 3 \cdot 5 \cdot 11 \cdot 13$$

What if we want to know which prime factors n and m have in common? How do we go about finding them? If we are able to factor the two numbers as we are with 561 and 2145 above, then we can just check which ones which they share. From above we can see that 561 and 2145 share 3 and 11 as common factors. But it's not always this easy to factor integers into primes [4]. To comprehend the difficulty of this task consider the number below whose nickname is RSA-2048.

25195908475657893494027183240048398571429282126204032027777137836043662020
70759555626401852588078440691829064124951508218929855914917618450280848912
00728449926873928072877767359714183472702618963750149718246911650776133798
59095700097330459748808428401797429100642458691817195118746121515172654632
28221686998754918242243363725908514186546204357679842338718477444792073993
42365848238242811981638150106748104516603773060562016196762561338441436038
33904414952634432190114657544454178424020924616515723350778707749817125772
46796292638635637328991215483143816789988504044536402352738195137863656439
1212010397122822120720357

RSA-2048 has 617 decimal digits and was part of a factoring challenge that ended in 2007. The number RSA-2048 is the product of only 2 prime numbers i.e.

$$\text{RSA-2048} = p \cdot q$$

Even the most powerful computers today can take months to factor certain integers over 200 digits long. Before the factoring challenge ended in 2007 the prize money for finding the factors p and q of RSA-2048 was a fifth of a million US dollars, but if you could factor this number today, the prize money would be a small fraction of what it would be worth. Anyways, back to what we were trying to do. What was it?

We were trying to find the prime numbers which divide both n and m. We know we can use the fundamental theorem of arithmetic, but as we have seen, FACTORING IS HARD! Is there another way of accomplishing the same objective? The answer is yes, and the way of doing it is called *the division algorithm.*

The division algorithm uses a simple fact in a clever way to accomplish a highly non-trivial goal. We are trying to find all the prime numbers which n and m share in their *prime factorization* given by the fundamental theorem of arithmetic. Suppose

[4]Indeed it is the difficulty of this problem that encrypts data and keeps online information safe. We will see more precisely how this works later.

p is a prime which divides both n and m. The simple fact is that p must divide the difference $n-m$. This is because if p is a factor of both n and m then we can write

$$\begin{aligned} n &= p \cdot a && \text{for some other integer } a \\ m &= p \cdot b && \text{for some other integer } b \end{aligned}$$

But then we have

$$\begin{aligned} n - m &= p \cdot a - p \cdot b \\ &= p \cdot (a - b) \end{aligned}$$

What does this last equality mean? It means precisely that the difference $n-m$ is divisible by p. To see how this works in our example with 561 and 2145 take p to be 11. Then

$$\begin{aligned} 2145 &= 11 \cdot 195 \\ 561 &= 11 \cdot 51 \end{aligned}$$

and the difference is

$$\begin{aligned} 2145 - 561 &= 1584 \\ &= 11 \cdot (195 - 51) \\ &= 11 \cdot 144 \end{aligned}$$

What if we switch the order of n and m? Why is the answer still the same? In the example we have

$$\begin{aligned} 561 - 2145 &= -1584 \\ &= 11 \cdot (51 - 195) \\ &= 11 \cdot (-144) \end{aligned}$$

So how does this help us find out what the value of p is if we don't know before hand like in the example? This process gives us a way to take two numbers n and m sharing a common divisor p and create a new number $n-m$ which is *strictly less than n or m* [5]. If we continue this process then where does it stop? Back to the example of trying to find the common factors of 561 and 2145.

$$\begin{aligned} 2145 - 561 &= 1584 \\ 1584 - 561 &= 1023 \\ 1023 - 561 &= 462 \end{aligned}$$

At this point in the algorithm we have found a number 462 which is smaller than both 561 and 2145 and which is also divisible by any common factor of 561 and 2145. How do we proceed now? We could subtract 561 from 462, but let us instead subtract 462 from 561 to keep the difference positive. As we saw before it doesn't

[5] The strict inequality is important. When one studies other objects resembling $\mathbb{Z}$ this is not always true, and in fact turns out to be a property that is quite rare. $\mathbb{Z}$ is special!

matter. Continuing in this manner we have

$$\begin{aligned}
561 - 462 &= 99\\
462 - 99 &= 363\\
363 - 99 &= 264\\
264 - 99 &= 165\\
165 - 99 &= 66\\
99 - 66 &= 33\\
66 - 33 &= 33\\
33 - 33 &= 0
\end{aligned}$$

At zero this process can go no further (or is it farther?). But zero doesn't help us find out what the common factors of 561 and 2145 are. So what's the deal? Did this algorithm do anything for us?

Exercise 2.7. Go back to where we wrote out the factors of 561 and 2145. Find the common factors of 561 and 2145. How do these common factors relate to the process we carried out which we called the division algorithm?

Exercise 2.8. A very observant student pipes up and says, "I thought this was called the division algorithm, all I see is subtraction?!?!" Is the division algorithm poorly named, or is this student missing something?

3. October 25 - October 31 2009

The Integers Modulo n (also known as $\mathbb{Z}/n\mathbb{Z}$).

References

[OA66] C. Stanley Ogilvy and John T. Anderson, *Excursions In Number Theory*, Dover, 1966.
[Ore67] O. Ore, *Invitation to number theory*, Mathematical Association of America, 1967.